



REPLY TO DES MOINES OFFICE

February 27, 2009

*VIA Electronic Comment Filing System*

Marlene H. Dortch, Secretary  
Office of the Secretary  
Federal Communications Commission  
445 12th Street, SW, Suite TW-A325  
Washington, DC 20554

**Re: EB Docket No. 06-36 - Annual CPNI Certification and  
Accompanying Statement**

Dear Ms. Dortch:

On February 18, 2009, an Annual CPNI Compliance Certification was filed by the undersigned on behalf of Northeast Iowa Telephone Company and its subsidiaries, pursuant to Commission Rule 64.2009(e). The filing was made via the Commission's Electronic Comment Filing System (ECFS). Upon review of the filing, it is apparent that the cover letter prepared in connection with the filing was omitted from the actual electronic submission.

In order to ensure compliance with the filing instructions issued by the Enforcement Bureau via Public Notice dated January 7, 2009, the compliance certification is being re-filed with this cover letter. If you have any questions or need further information, please contact the undersigned at (515) 288-2500 or via e-mail at [JohnPietila@davisbrownlaw.com](mailto:JohnPietila@davisbrownlaw.com).

Sincerely,

DAVIS, BROWN, KOEHN, SHORS & ROBERTS, P.C.

/s/

*John C. Pietila*

Attachments  
- Certification as Previously Filed

#1655772

DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

John D. Shors  
Stephen W. Roberts  
William R. King  
Robert F. Holz, Jr.  
Robert A. Gamble  
Michael G. Kulik  
Frank J. Carroll  
Bruce I. Campbell  
Jonathan C. Wilson  
Steven L. Nelson  
David B. VanSickel  
Gene R. La Suer  
Deborah M. Tharnish  
Kent A. Herink  
Robert J. Douglas, Jr.  
Mark D. Walz  
Gary M. Myers  
Stanley J. Thompson  
David A. Tank  
David M. Erickson  
Lori Torgerson Chesser  
Jo Ellen Whitney  
Becky S. Knutson  
Julie Johnson McLean  
Beverly Evans  
Margaret Van Houten  
Christopher P. Jannes  
Sharon K. Malheiro  
Kris Holub Tilley  
William A. Boatwright  
Thomas J. Houser  
Kendall R. Watkins  
Scott M. Brennan  
Debra Rectenbaugh Pettit  
Matthew E. Laughlin  
Judith R. Lynn Boes  
William P. Kelly  
Susan J. Freed  
Jason M. Ross  
Jason M. Stone  
Amy M. Landwehr  
John C. Pietila  
Emily E. Harris  
B. J. Miller  
Jeffrey D. Ewoldt  
Jodie L. Clark  
John S. Long  
Tara Z. Hall  
Charles N. Wittmack  
Courtney Strutt Todd  
Scott D. Mikkelsen  
Kelly A. Deters  
Amber K. Rutledge  
Nichole Miras Mordini  
Krystle L. Campa  
Sarah K. Franklin  
Victoria P. Nwasike  
M. Michelle Lickteig

Intellectual Property  
Kent A. Herink  
Emily E. Harris

Of Counsel  
Donald J. Brown  
Denise R. Claton  
C. Carleton Frederici  
A. J. Greffenius  
Dennis D. Jerde  
William J. Koehn  
Joseph M. Pawlosky  
Richard E. Ramsay  
Thomas E. Salsbery  
Neal Smith  
William D. Thomas

A. Arthur Davis  
1928-1997

ANNUAL 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2008

Date Filed: February 18, 2009

Name of Company(s) Covered by this Certification:

Company Name	Form 499 Filer ID
Northeast Iowa Telephone Company	804732
NEIT Mobile, LLC	825786
NEIT Wireless, LLC	825785

Name of Signatory: David Byers

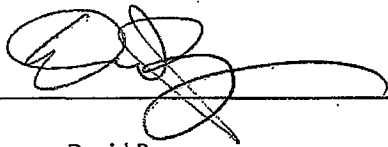
Title of Signatory: Assistant Secretary and General Manager

I, David Byers, acting as an agent of the companies identified above, certify that I am an officer of the companies and that I have personal knowledge that the companies have established operating procedures that are adequate to ensure that the companies are in compliance with the Commission's CPNI rules, including all requirements set forth in 47 C.F.R. § 64.2001 *et. seq.*

Attached to this certification is an accompanying statement explaining how the companies' operating procedures ensure that the companies are in compliance with the requirements set forth in the Commission's CPNI rules, including all requirements set forth in 47 C.F.R. § 64.2001 *et. seq.*

The companies have not taken any actions against data brokers in the past year. The companies will report any information they may obtain with respect to the processes pretexters are using to attempt to access CPNI and what steps the companies are taking to protect CPNI.

The companies have not received any customer complaints in the past year concerning the unauthorized, use, disclosure or release of CPNI.

  
\_\_\_\_\_

Name: David Byers

Title: Assistant Secretary and General Manager

## ACCOMPANYING STATEMENT

This statement accompanies the Annual 64.2009(e) CPNI Certification for 2008 filed with the Commission on behalf of Northeast Iowa Telephone Company, an Iowa corporation and its wholly owned subsidiaries, NEIT Mobile, LLC an Iowa limited liability company and NEIT Wireless, LLC, an Iowa limited liability company (collectively, the "Company"). The Company's operating procedures ensure that the Company is in compliance with the requirements set forth in the Commission's CPNI rules as set forth in 47 C.F.R. Part 64, Subpart U (the "CPNI Rules") as follows:

- The Company's operating procedures prohibit the use, disclosure or release of CPNI, except as permitted or required under 47 U.S.C. § 222(d) and Rule 64.2005. The Company does not use disclose or permit access to CPNI for any purpose (including marketing communications-related services) and does not disclose or grant access to CPNI to any party (including to agents or affiliates that provide communications-related services), except as permitted under 47 U.S.C. § 222(d) and Rule 64.2005.
- The Company's operating procedures prohibit the use of CPNI in sales or marketing campaigns. The Company does not use, disclose or grant access to CPNI for any purpose, to any party or in any manner that would require a customer's "opt in" or "opt out" approval under the Commission's CPNI Rules. The Company does not currently solicit "opt in" or "opt out" customer approval for the use or disclosure of CPNI.
- The Company takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. The Company's operating procedures include safeguards designed to identify and protect against unauthorized use, disclosure or access to CPNI. The Company authenticates a customer in accordance with the Commission's CPNI rules prior to disclosing CPNI based on customer-initiated telephone contact or an in-store visit.
- The Company maintains a record of all instances where CPNI was disclosed or provided to third parties and where third parties were permitted access to CPNI. Records of all instances where CPNI was disclosed or provided to third parties, or where third parties were permitted access to CPNI, are maintained for a minimum of one year.
- The Company does not release call detail CPNI over the telephone, based on customer-initiated telephone contact, unless the customer first provides a password that is not prompted by the Company asking for readily available biographical information or account information or unless the customer is able to provide the relevant call detail information without Company assistance. If a customer does not provide a password and is not able to provide the relevant call detail information without Company assistance, the Company only discloses call detail CPNI by sending it to an address of record or by calling the customer at the telephone number of record.
- The Company provides customers with access to CPNI at the Company's retail locations only if the customer presents a valid photo ID and the valid photo ID matches an authorized name on the customer account. If a customer is not able to provide a valid photo ID, he or she may instead provide the account password in the same manner required for customer-initiated telephone contact. If a customer is not able to provide a valid photo ID or account password in connection with an in person inquiry, the Company only discloses call detail CPNI by sending it to an address of record or by calling the customer at the telephone number of record.

NORTHEAST IOWA TELEPHONE COMPANY AND SUBSIDIARIES  
Annual 64.2009(e) CPNI Certification for 2008  
February 18, 2009

- The Company has established a system of passwords and password protection. For a new customer establishing service, the Company requests that the customer establish a password at the time of service initiation. For existing customers to establish a password, the Company must first authenticate the customer without the use of readily available biographical information or account information, for example by calling the customer at the telephone number of record or by using a personal identification number (PIN) or similar method to authenticate a customer.
- If a customer password is forgotten or lost, the Company uses a backup customer authentication method that is not based on readily available biographical information or account information.
- If a customer does not want to establish a password or if a password is lost or forgotten without subsequent authentication of the customer, the customer may only access call detail information based on a customer-initiated telephone call by asking the Company to send the call detail information to an address of record or by the Company calling the customer at the telephone number of record. If a customer does not want to establish a password or if a password is lost or forgotten without subsequent authentication of the customer, the customer may only access call detail information based on personal inquiry at a retail location by providing a valid photo ID that matches an authorized name on the customer account or by asking the Company to send the call detail information to an address of record or by the Company calling the customer at the telephone number of record.
- The Company has procedures and policies in place to notify a customer immediately when a password, customer response to a back-up means of authentication, address of record or other critical account information is created or changed.
- The Company does not currently provide online account access to customers.
- All Company employees with access to or a need to use CPNI have been trained regarding the Company's operating procedures and as to when they are and are not authorized to use, disclose or permit access to CPNI. The Company's employees have been trained regarding the types of information that constitute CPNI and the Company's safeguards (such as employee restrictions, password protection, supervisory review, etc.) applicable to the Company's handling of CPNI. The Company's employee manual includes a disciplinary policy requiring compliance with the Company's operating procedures and sets forth penalties for non-compliance, up to and including termination of employment.
- The Company has appointed a compliance officer and established a supervisory review process regarding the Company's compliance with the Commission's CPNI Rules. The Company's operating policies require that employees confer with the compliance officer if they are unsure about any circumstances or situations involving the potential use, disclosure or release of CPNI. The Company's operating policies require that the compliance officer confer with the Company's legal counsel if he or she is unsure about any circumstances or situations involving the potential use, disclosure or release of CPNI.

NORTHEAST IOWA TELEPHONE COMPANY AND SUBSIDIARIES  
Annual 64.2009(e) CPNI Certification for 2008  
February 18, 2009

- The Company's compliance officer has personal knowledge of the Company's operating procedures and is authorized, as an agent of the Company, to sign and file an annual CPNI compliance certification with the Commission.
- All Company employees and the compliance officer are trained to identify and protect against activity that is indicative of pretexting. All Company employees and the compliance officer are required to report any breach or potential breach of CPNI safeguards and/or any customer complaints regarding CPNI. In the event of a CPNI breach, the Company's operating procedures require compliance with the Commission's CPNI Rules regarding notice to law enforcement and customers. The Company must maintain records of any discovered breaches and notifications to the Secret Service and the FBI regarding those breaches, as well as the Secret Service and the FBI responses to such notifications, for a period of at least two years.